

## Amendment

U.S. Divisional Application of KATO et al., atty. dkt. 290460

10/035,311

information that changes each time the data is reproduced, such as time information.

Therefore, even when the data flowing the CPU BUS 110 is stored from signal lines 210 into a digital storage medium 211 as shown in Fig. 4, the data cannot be reproduced or used.--

Page 27, please replace the paragraph beginning with line 3 with the following paragraph:

--In the second embodiment, there is an  $n$  number of types of master keys. A first session key is represented by  $S_K$ , a second session key by  $S_{K'}$ , the  $t$ -th master key  $M_{Kt}$  ( $t$  is in the range of 1 to  $n$ ), and image data (i.e., the data to be enciphered) Data.--

Page 28, please replace the paragraphs beginning with lines 2, 6, <sup>10 19</sup>~~N~~, ~~2Q~~ and 25 with the following paragraphs, respectively:

--(Method 1) One session key  $E_{MKi}(S_K)$  ( $i$  is in the range of 1 to  $n$ ) is recorded on the DVD 101. The deciphering unit 114a has an  $n$  number of master keys  $M_{Kj}$  ( $j = 1$  to  $n$ ) in it.--

--(Method 2) An  $n$  number of session keys  $E_{MKi}(S_K)$  ( $i = 1$  to  $n$ ) are recorded on the DVD 101. The deciphering unit 114a has one master key  $M_{Kj}$  ( $j$  is in the range of 1 to  $n$ ) in it.--

--(Method 3) This is an expansion of Method 2. An  $n$  number of session keys  $E_{MKi}(S_K)$  ( $i = 1$  to  $n$ ) are recorded on the DVD 101. The deciphering unit 114a has an  $m$  ( $2 < m < n$ ) number of master keys  $M_{Kj}$  ( $j = 1$  to  $n$ ) in it. The  $m$  number of master keys have been selected from the  $n$  number of master keys beforehand.--

--(Method 4) This is the reverse of Method 3. An  $m$  ( $2 < m < n$ ) number of session keys  $E_{MKi}(S_K)$  ( $i = 1$  to  $n$ ) are recorded on the DVD 101. The  $m$  number of master keys have been selected from an  $n$  number of master keys  $M_{Kj}$  ( $j = 1$  to  $n$ ) beforehand. The deciphering unit 114a has an  $n$  number of master keys  $M_{Kj}$  ( $j = 1$  to  $n$ ) in it.--